The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

07/29/2014

SUBJECT:

Multiple Security Vulnerabilities Reported in Siemens SIMATIC WinCC

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in the Siemen's Supervisory Control and Data Acquisition (SCADA) system, SIMATIC WinCC, which could allow unauthorized escalation of user privileges. SIMATIC WinCC is a SCADA system that is used to monitor and control physical processes involved in industry and infrastructure. This software is used in many industries, including food and beverage, water and wastewater, oil and gas, and chemical. Successful exploitation of these vulnerabilities could allow an attacker access to sensitive information or allow a user to gain privileges. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

All versions of SIMATIC WinCC prior to version 7.3
All versions of SIMATIC PCS7 (as WinCC is incorporated) prior to version 8.1

RISK:

Government:

Large and medium government entities: **High**
Small government entities: **High**

Businesses:

Large and medium business entities: **High**
Small business entities: **High**
Home users: N/A

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in SIMATIC WinCC. Details of these vulnerabilities are as follows:

An unauthenticated remote attacker could obtain sensitive information via a specially crafted HTTP or HTTPS request to the SIMATIC WinCC WebNavigator server. [CVE-2014-4682]
A remote authenticated user could escalate their privileges without authorization via the existing access control settings. [CVE-2014-4683]
A remote authenticated user could escalate their privileges in the SIMATIC WinCC database without authorization via a specially crafted request to TCP port 1433. [CVE-2014-4684]
A local user could obtain limited escalated privileges within the operating system by leveraging a weak system-object access control. [CVE-2014-4685]
An unauthorized disclosure of information is caused by a hard-coded cryptographic key. This could allow for an escalation of privileges if network communication on TCP port 1030 of a legitimate user can be captured. [CVE-2014-4686]

RECOMMENDATIONS:

The following actions should be taken:

Upgrade to SIMATIC WinCC v7.3 as these vulnerabilities have been mitigated in this version.
White list trusted networks and clients.
Only allow trusted traffic over TCP port 1433.
Deactivate all unnecessary users on the WinCC server.

REFERENCES:

Security Focus:

http://www.securityfocus.com/bid/68880

http://www.securityfocus.com/bid/68876

http://www.securityfocus.com/bid/68879

http://www.securityfocus.com/bid/68872

http://www.securityfocus.com/bid/68875

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4682

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4683

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4684

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4685

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4686

ICS-CERT:

https://ics-cert.us-cert.gov/advisories/ICSA-14-205-02